

In the claims:

This listing of claims will replace all prior versions and listings of claims in the application:

1 1. (currently amended) ~~[[The]]~~ A method for mutual authentication of a first station and a second
2 station, comprising:

3 ~~encrypting~~ providing a particular data random key at the first station, disassembling and
4 ~~by first~~ veiling the particular data random key ~~[[using]]~~ by forming a first conversion array
5 seeded by a shared secret and then encrypting the first conversion array ~~veiled particular data~~
6 ~~random key~~ to produce a first encrypted data set ~~[[key]]~~, where access to the shared secret
7 indicates authenticity of the first station;

8 sending a first message to the second station including the first encrypted data set ~~[[key]]~~,
9 where the second station decrypts first encrypted data set and unveils and reassembles said
10 particular data random key using the shared secret, and where the second station disassembles
11 and veils ~~encrypts the particular data random key by first veiling~~ a version of the particular data
12 random key ~~[[using]]~~ by forming a second conversion array seeded by the shared secret and then
13 ~~encrypting~~ encrypts the ~~veiled~~ second conversion array ~~version of the particular data random key~~
14 to produce a second encrypted key, and sends a second message to the first station carrying the
15 second encrypted data set ~~[[key]]~~, where access to the shared secret indicates authenticity of the
16 second station; ~~[[and]]~~

17 receiving the second message, and decrypting the second encrypted data set, and
18 reassembling and unveiling the version of the particular data random key at the first station; and

19 determining at the first station if the version of the particular data random key matches an
20 expected version the particular data random key, and if so providing an additional particular data
21 random key at the first station, disassembling and veiling the additional particular data random
22 key by forming a third conversion array seeded by an additional shared secret and then
23 encrypting the third conversion array to produce a first additional encrypted data set, where
24 access to the additional shared secret indicates authenticity of the first station;

25 sending a third message to the second station including the first additional encrypted data
26 set, where the second station decrypts the first additional encrypted data set and reassembles and
27 unveils said additional particular data random key using the additional shared secret, and where

28 the second station disassembles and veils a version of the additional particular data random key
29 by forming a fourth conversion array seeded by the additional shared secret and then encrypts the
30 fourth conversion array to produce a second additional encrypted data set, and sends a fourth
31 message to the first station carrying the second additional encrypted data set, where access to the
32 additional shared secret indicates authenticity of the second station; and
33 receiving the fourth message, and decrypting the second additional encrypted data set and
34 reassembling and unveiling the version of the additional particular data random key at the first
35 station, and
36 determining at the first station if the version of the additional data random key matches
37 an expected version the additional data random key, and if so continuing with further exchanges
38 of messages with the second station.

1 2. (canceled).

1 3. (currently amended) The method of claim 1 [[2]], wherein said additional particular data
2 random key is the same as the particular data random key.

1 4. (currently amended) The method of claim 1, where the one of the first and second conversion
2 arrays comprises X sections, each of said X sections including Y byte positions in an order, and
3 including instructions
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a pseudorandom number having X values
6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions, and
8 placing a byte of said random key in each of said X sections at the one of said Y byte
9 positions identified by the corresponding one of said X values.

1 5. (withdrawn) The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Z bit positions in an order, and including
3 generating one of the first and second conversion arrays using a random number
4 generator seeded by said shared secret to produce a pseudorandom number having X values

5 corresponding with respective sections of said X sections, the X values each being between 1 and
6 Z and identifying one of said Z bit positions, and
7 placing a bit of said random key in each of said X sections at the one of said Z bit
8 positions identified by the corresponding one of said X values.

1 6. (withdrawn) The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each of said
3 Y byte positions including B bit positions in an order, and including
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a first pseudorandom number having X values
6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions,
8 using a random number generator seeded by said shared secret to produce a second
9 pseudorandom number having B values corresponding with respective bits in a byte of said
10 random key, the B values each being between 1 and B and identifying one of said B bit positions,
11 placing a byte, including B bits, of said random key in each of said X sections at the one
12 of said Y byte positions identified by the corresponding one of said X values, and
13 mapping the B bits of said byte of said random key to said B bit positions identified by
14 the corresponding one of said B values.

1 7. (withdrawn) The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each of said
3 Y byte positions including B bit positions in an order, and including
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a first pseudorandom number having X values
6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions,
8 using a random number generator to produce a second pseudorandom number having B
9 values corresponding with respective bits in a byte of said random key, the B values each being
10 between 1 and B and identifying one of said B bit positions,

11 placing a byte, including B bits, of said random key in each of said X sections at the one
12 of said Y byte positions identified by the corresponding one of said X values, and
13 mapping the B bits of said byte of said random key to said B bit positions identified by
14 the corresponding one of said B values.

1 8. (currently amended) The method of claim 1, including presenting a ~~[[use]]~~ user interface to
2 the second station from the first station carrying parameters of said first and second conversion
3 arrays.

1 9. (original) The method of claim 1, including executing an interactive exchange of messages to
2 deliver the particular data random key from the first station to the second station.

1 10. (currently amended) A data processing apparatus, comprising:

2 a processor, a communication interface adapted for connection to a communication
3 medium, and memory storing instructions for execution by the data processor, the instructions
4 including

5 logic to ~~encrypt~~ provide a particular data random key at the first station and to
6 disassemble and veil ~~by first veiling~~ the particular data random key ~~[[using]]~~ by forming a first
7 conversion array seeded by a shared secret and then to encrypt the first conversion array ~~veiled~~
8 ~~particular data random key~~ to produce a first encrypted data set key, where access to the shared
9 secret indicates authenticity of the first station;

10 logic to send a first message to the second station including the first encrypted data set
11 ~~[[key]]~~, where the second station decrypts and unveils the first encrypted data set ~~said particular~~
12 ~~data random key~~ using the shared secret, and where the second station ~~encrypts the particular~~
13 ~~data random key by first veiling~~ disassembles and veils a version of the particular data random
14 key ~~using~~ by forming a second conversion array seeded by the shared secret and then to encrypt
15 ~~encrypting the veiled version of the particular data random key~~ second conversion array to
16 produce a second encrypted data set ~~[[key]]~~, and sends a second message to the first station
17 carrying the second encrypted data set ~~[[key]]~~, where access to the shared secret indicates
18 authenticity of the second station; ~~[[and]]~~

19 logic to receive the second message, and to decrypt and unveil the version of the
20 particular data random key at the first station; and
21 logic to determine at the first station if the version of the particular data random key
22 matches an expected version the particular data random key, and if so provide an additional
23 particular data random key at the first station, disassemble and veil the additional particular data
24 random key by forming a third conversion array seeded by an additional shared secret and then
25 to encrypt the third conversion array to produce a first additional encrypted data set, where
26 access to the additional shared secret indicates authenticity of the first station;
27 logic to send a third message to the second station including the first additional encrypted
28 data set, where the second station decrypts the first additional encrypted data set and reassembles
29 and unveils the additional particular data random key using the additional shared secret, and
30 where the second station disassembles and veils a version of the additional particular data
31 random key by forming a fourth conversion array seeded by the additional shared secret and then
32 encrypts the fourth conversion array to produce a second additional encrypted data set, and sends
33 a fourth message to the first station carrying the second additional encrypted data set, where
34 access to the additional shared secret indicates authenticity of the second station;
35 logic to receive the fourth message, and decrypt the second additional encrypted data set
36 and to reassemble and unveil the version of the additional particular data random key at the first
37 station; and
38 logic to determine at the first station if the version of the additional data random key
39 matches an expected version the additional data random key, and if so to continue with further
40 exchanges of messages with the second station.

1 11. (canceled).

1 12. (currently amended) The apparatus of claim 10 [[11]], wherein said additional particular data
2 random key is the same as the particular data random key.

1 13. (original) The apparatus of claim 10, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, and
3 including logic to

4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a pseudorandom number having X values corresponding
6 with respective sections of said X sections, the X values each being between 1 and Y and
7 identifying one of said Y byte positions, and
8 to place a byte of said random key in each of said X sections at the one of said Y byte
9 positions identified by the corresponding one of said X values.

1 14. (withdrawn) The apparatus of claim 10, where the one of the first and second conversion
2 arrays comprises X sections, each of said X sections including Z bit positions in an order, and
3 including logic to

4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a pseudorandom number having X values corresponding
6 with respective sections of said X sections, the X values each being between 1 and Z and
7 identifying one of said Z bit positions, and
8 to place a bit of said random key in each of said X sections at the one of said Z bit
9 positions identified by the corresponding one of said X values.

1 15. (withdrawn) The apparatus of claim 10, where the one of the first and second conversion
2 arrays comprises X sections, each of said X sections including Y byte positions in an order, each
3 of said Y byte positions including B bit positions in an order, and including logic to

4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a first pseudorandom number having X values
6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions,

8 use a random number generator seeded by said shared secret to produce a second
9 pseudorandom number having B values corresponding with respective bits in a byte of said
10 random key, the B values each being between 1 and B and identifying one of said B bit positions,

11 place a byte, including B bits, of said random key in each of said X sections at the one of
12 said Y byte positions identified by the corresponding one of said X values, and

13 map the B bits of said byte of said random key to said B bit positions identified by the
14 corresponding one of said B values.

1 16. (withdrawn) The apparatus of claim 10, where the one of the first and second conversion
2 arrays comprises X sections, each of said X sections including Y byte positions in an order, each
3 of said Y byte positions including B bit positions in an order, and including logic to
4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a first pseudorandom number having X values
6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions,
8 use a random number generator to produce a second pseudorandom number having B
9 values corresponding with respective bits in a byte of said random key, the B values each being
10 between 1 and B and identifying one of said B bit positions,
11 place a byte, including B bits, of said random key in each of said X sections at the one of
12 said Y byte positions identified by the corresponding one of said X values, and
13 map the B bits of said byte of said random key to said B bit positions identified by the
14 corresponding one of said B values.

1 17. (original) The apparatus of claim 10, including logic to present a user interface to the second
2 station from the first station carrying parameters of said first and second conversion arrays.

1 18. (original) The apparatus of claim 10, including logic to execute an interactive exchange of
2 messages to deliver the particular data random key from the first station to the second station.

1 19. (currently amended) An article, comprising:
2 machine readable data storage medium having computer program instructions stored
3 therein for establishing a communication session on a communication medium between a first
4 data processing station and a second data processing station having access to the communication
5 medium, said instructions comprising
6 logic to ~~encrypt~~ provide a particular data random key at the first station and to
7 disassemble and veil ~~by first veiling~~ the particular data random key ~~using~~ by forming a first
8 conversion array seeded by a shared secret and then to encrypt the first conversion array veiled
9 ~~particular data random key~~ to produce a first encrypted data set [[key]], where access to the
10 shared secret indicates authenticity of the first station;

11 logic to send a first message to the second station including the first encrypted data set
12 key, where the second station decrypts and unveils the first encrypted data set ~~said particular data~~
13 ~~random key~~ using the shared secret, and where the second station ~~encrypts the particular data~~
14 ~~random key by first veiling~~ disassembles and veils a version of the particular data random key
15 using by forming a second conversion array seeded by the shared secret and then to encrypt
16 encrypting the veiled version of the particular data random key second conversion array to
17 produce a second encrypted data set [[key]], and sends a second message to the first station
18 carrying the second encrypted data set [[key]], where access to the shared secret indicates
19 authenticity of the second station; [[and]]

20 logic to receive the second message, and to decrypt and unveil the version of the
21 particular data random key at the first station; and

22 logic to determine at the first station if the version of the particular data random key
23 matches an expected version the particular data random key, and if so provide an additional
24 particular data random key at the first station, disassemble and veil the additional particular data
25 random key by forming a third conversion array seeded by an additional shared secret and then
26 to encrypt the third conversion array to produce a first additional encrypted data set, where
27 access to the additional shared secret indicates authenticity of the first station;

28 logic to send a third message to the second station including the first additional encrypted
29 data set, where the second station decrypts the first additional encrypted data set and reassembles
30 and unveils the additional particular data random key using the additional shared secret, and
31 where the second station disassembles and veils a version of the additional particular data
32 random key by forming a fourth conversion array seeded by the additional shared secret and then
33 encrypts the fourth conversion array to produce a second additional encrypted data set, and sends
34 a fourth message to the first station carrying the second additional encrypted data set, where
35 access to the additional shared secret indicates authenticity of the second station;

36 logic to receive the fourth message, and decrypt the second additional encrypted data set
37 and to reassemble and unveil the version of the additional particular data random key at the first
38 station; and

39 logic to determine at the first station if the version of the additional data random key
40 matches an expected version the additional data random key, and if so to continue with further
41 exchanges of messages with the second station.

1 20. (canceled).

1 21. (original) The article of claim 19, wherein said additional particular data random key is the
2 same as the particular data random key.

1 22. (original) The article of claim 19, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, and the
3 instructions include logic to
4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a pseudorandom number having X values corresponding
6 with respective sections of said X sections, the X values each being between 1 and Y and
7 identifying one of said Y byte positions, and
8 to place a byte of said random key in each of said X sections at the one of said Y byte
9 positions identified by the corresponding one of said X values.

1 23. (withdrawn) The article of claim 19, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Z bit positions in an order, and the
3 instructions include logic to
4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a pseudorandom number having X values corresponding
6 with respective sections of said X sections, the X values each being between 1 and Z and
7 identifying one of said Z bit positions, and
8 to place a bit of said random key in each of said X sections at the one of said Z bit
9 positions identified by the corresponding one of said X values.

1 24. (withdrawn) The article of claim 19, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each of said
3 Y byte positions including B bit positions in an order, and the instructions include logic to
4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a first pseudorandom number having X values

6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions,
8 use a random number generator seeded by said shared secret to produce a second
9 pseudorandom number having B values corresponding with respective bits in a byte of said
10 random key, the B values each being between 1 and B and identifying one of said B bit positions,
11 place a byte, including B bits, of said random key in each of said X sections at the one of
12 said Y byte positions identified by the corresponding one of said X values, and
13 map the B bits of said byte of said random key to said B bit positions identified by the
14 corresponding one of said B values.

1 25. (withdrawn) The article of claim 19, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each of said
3 Y byte positions including B bit positions in an order, and the instructions include logic to
4 generate one of the first and second conversion arrays using a random number generator
5 seeded by said shared secret to produce a first pseudorandom number having X values
6 corresponding with respective sections of said X sections, the X values each being between 1 and
7 Y and identifying one of said Y byte positions,
8 use a random number generator to produce a second pseudorandom number having B
9 values corresponding with respective bits in a byte of said random key, the B values each being
10 between 1 and B and identifying one of said B bit positions,
11 place a byte, including B bits, of said random key in each of said X sections at the one of
12 said Y byte positions identified by the corresponding one of said X values, and
13 map the B bits of said byte of said random key to said B bit positions identified by the
14 corresponding one of said B values.

1 26. (original) The article of claim 19, wherein the instructions include logic to present a user
2 interface to the second station from the first station carrying parameters of said first and second
3 conversion arrays.

1 27. (original) The article of claim 19, wherein the instructions include logic to execute an
2 interactive exchange of messages to deliver the particular data random key from the first station
3 to the second station.

1 28. (new) A method for mutual authentication of a first station and a second station, comprising:
2 providing a particular data random key at the first station, disassembling and veiling the
3 particular data random key by forming a first conversion array seeded by a shared secret and then
4 encrypting the first conversion array to produce a first encrypted data set, where access to the
5 shared secret indicates authenticity of the first station;
6 sending a first message to the second station including the first encrypted data set ~~key~~,
7 where the second station decrypts first encrypted data set and unveils and reassembles said
8 particular data random key using the shared secret, and where the second station disassembles
9 and veils a version of the particular data random key by forming a second conversion array
10 seeded by the shared secret and then encrypts the second conversion array to produce a second
11 encrypted key, and sends a second message to the first station carrying the second encrypted data
12 set, where access to the shared secret indicates authenticity of the second station;
13 receiving the second message, and decrypting the second encrypted data set, and
14 reassembling and unveiling the version of the particular data random key at the first station; and
15 determining at the first station if the version of the particular data random key matches an
16 expected version the particular data random key, and if so continuing with further exchanges of
17 messages with the second station;
18 where the one of the first and second conversion arrays comprises X sections, each of
19 said X sections including Y byte positions in an order, and including
20 generating one of the first and second conversion arrays using a random number
21 generator seeded by said shared secret to produce a pseudorandom number having X values
22 corresponding with respective sections of said X sections, the X values each being between 1 and
23 Y and identifying one of said Y byte positions, and
24 placing a byte of said random key in each of said X sections at the one of said Y byte
25 positions identified by the corresponding one of said X values.

1 29. (new) A data processing apparatus, comprising:
2 a processor, a communication interface adapted for connection to a communication
3 medium, and memory storing instructions for execution by the data processor, the instructions
4 including
5 logic to provide a particular data random key at the first station and to disassemble and
6 veil the particular data random key by forming a first conversion array seeded by a shared secret
7 and then to encrypt the first conversion array to produce a first encrypted data set, where access
8 to the shared secret indicates authenticity of the first station;
9 logic to send a first message to the second station including the first encrypted data set
10 key, where the second station decrypts and unveils the first encrypted data set using the shared
11 secret, and where the second station disassembles and veils a version of the particular data
12 random key by forming a second conversion array seeded by the shared secret and then to
13 encrypt the second conversion array to produce a second encrypted data set, and sends a second
14 message to the first station carrying the second encrypted data set, where access to the shared
15 secret indicates authenticity of the second station;
16 logic to receive the second message, and to decrypt and unveil the version of the
17 particular data random key at the first station; and
18 logic to determine at the first station if the version of the particular data random key
19 matches an expected version the particular data random key, and if so to continue with further
20 exchanges of messages with the second station;
21 where the one of the first and second conversion arrays comprises X sections, each of
22 said X sections including Y byte positions in an order, and including logic to
23 generate one of the first and second conversion arrays using a random number generator
24 seeded by said shared secret to produce a pseudorandom number having X values corresponding
25 with respective sections of said X sections, the X values each being between 1 and Y and
26 identifying one of said Y byte positions, and
27 to place a byte of said random key in each of said X sections at the one of said Y byte
28 positions identified by the corresponding one of said X values.

1 30. (new) An article, comprising:

2 machine readable data storage medium having computer program instructions stored
3 therein for establishing a communication session on a communication medium between a first
4 data processing station and a second data processing station having access to the communication
5 medium, said instructions comprising

6 logic to provide a particular data random key at the first station and to disassemble and
7 veil the particular data random key by forming a first conversion array seeded by a shared secret
8 and then to encrypt the first conversion array to produce a first encrypted data set, where access
9 to the shared secret indicates authenticity of the first station;

10 logic to send a first message to the second station including the first encrypted data set
11 key, where the second station decrypts and unveils the first encrypted data set using the shared
12 secret, and where the second station disassembles and veils a version of the particular data
13 random key by forming a second conversion array seeded by the shared secret and then to
14 encrypt the second conversion array to produce a second encrypted data set, and sends a second
15 message to the first station carrying the second encrypted data set, where access to the shared
16 secret indicates authenticity of the second station;

17 logic to receive the second message, and to decrypt and unveil the version of the
18 particular data random key at the first station; and

19 logic to determine at the first station if the version of the particular data random key
20 matches an expected version the particular data random key, and if so to continue with further
21 exchanges of messages with the second station;

22 where the one of the first and second conversion arrays comprises X sections, each of
23 said X sections including Y byte positions in an order, and the instructions include logic to

24 generate one of the first and second conversion arrays using a random number generator
25 seeded by said shared secret to produce a pseudorandom number having X values corresponding
26 with respective sections of said X sections, the X values each being between 1 and Y and
27 identifying one of said Y byte positions, and

28 to place a byte of said random key in each of said X sections at the one of said Y byte
29 positions identified by the corresponding one of said X values.

31. (new) A method for mutual authentication of a first station and a second station, comprising:

- providing a particular data random key at the first station, disassembling and veiling the particular data random key by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array to produce a first encrypted data set ~~key~~, where access to the shared secret indicates authenticity of the first station;
- sending a first message to the second station including the first encrypted data set, where the second station decrypts first encrypted data set and unveils and reassembles said particular data random key using the shared secret;
- receiving the first message at the second station and decrypting the first encrypted data set, and reassembling and unveiling the particular data random key at the second station; and
- determining at the second station if the particular data random key matches an expected version the particular data random key, and if so and disassembling and veiling a version of the particular data random key by forming a second conversion array seeded by the shared secret and then encrypting the second conversion array to produce a second encrypted key, and sending a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;
- receiving the second message at the first station, and decrypting the second encrypted data set, and reassembling and unveiling the version of the particular data random key at the first station; and
- determining at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so providing an additional particular data random key at the first station, disassembling and veiling the additional particular data random key by forming a third conversion array seeded by an additional shared secret and then encrypting the third conversion array to produce a first additional encrypted data set, where access to the additional shared secret indicates authenticity of the first station;
- sending a third message to the second station including the first additional encrypted data set;
- receiving the third message at the second station and decrypting the first additional encrypted data set and unveiling and reassembling the additional particular data random key using the additional shared secret, and determining at the second station if the additional particular data random key matches an expected version the additional particular data random

32 key, and if so disassembling and veiling a version of the additional particular data random key by
33 forming a fourth conversion array seeded by the additional shared secret and then encrypting the
34 fourth conversion array to produce a second additional encrypted data set;
35 sending a fourth message to the first station carrying the second additional encrypted data
36 set, where access to the additional shared secret indicates authenticity of the second station;
37 receiving the fourth message, and decrypting the second additional encrypted data set and
38 unveiling and reassembling the version of the additional particular data random key at the first
39 station; and
40 determining at the first station if the version of the additional data random key matches
41 an expected version the additional data random key, and if so continuing with further exchanges
42 of messages with the second station.

///